AMENDMENT TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS

1. (Currently Amended) A handling device of security data comprising:

an in-vehicle unit having a portable unit authenticating unit, a nonvolatile memory, and a controller;

a vehicle having the in-vehicle unit, an in-vehicle system, and a communication unit; and

a portable unit gives ~~for giving~~ a control instruction to the in-vehicle system of the vehicle through communication with the communication unit,

wherein the portable unit transmits a signal indicating a [[the]] ID of the portable unit to the vehicle,

the communication unit receives the transmission signal,

the portable unit authenticating unit authenticates as to whether the signal is a transmission signal that is transmitted from a predetermined portable unit based on a comparison between the reception signal and data indicating the ID of the portable unit stored in the nonvolatile memory or not,

the controller ~~control unit~~ causes the in-vehicle system to perform the control instructions if the portable unit authenticating unit judges that the signal is a transmission signal that is transmitted from a predetermined portable unit,

an encryption unit for encrypting security data of the vehicle with a second cipher key is interposed between the controller and the nonvolatile memory of the in-vehicle unit, and

the security data is encrypted by the encryption unit with the second cipher key and stored into the nonvolatile memory according to an [[the]] instruction from the controller when the in-vehicle unit is set into a security data register mode.

2. (Currently Amended) The handling device of security data, according to Claim 1, wherein the second cipher key is stored in another nonvolatile memory that is different from the nonvolatile memory storing the encrypted signal of the security data.

3. (Previously Presented) The handling device of security data, according to Claim 2, wherein the security data includes a portable unit ID, the nonvolatile memory is an EEPROM, and another nonvolatile memory is a ROM.

4. (Previously Presented) The handling device of security data, according to Claim 3, wherein an in-vehicle unit ID is stored in the EEPROM in addition to the portable unit ID.

5. (Currently Amended) A handling method of security data of a vehicle provided with an in-vehicle unit having a portable unit authenticating unit, a first nonvolatile memory, and a controller, a vehicle having the in-vehicle unit, a door locking mechanism, and a communication unit, and a portable unit for locking or unlocking a door locking mechanism of the vehicle through communication with the communication unit, the method comprising:

transmitting, from the portable unit, instructions for locking/ unlocking the door locking mechanism of the vehicle and a signal indicating a [[the]] ID of the portable unit; and

receiving the signal by the communication unit provided in the vehicle;

the portable unit authenticating unit authenticating as to whether the signal is a transmission signal that is transmitted from a predetermined portable unit based on a comparison between data indicating the ID of the portable unit stored in the [[tine]] nonvolatile memory and data indicating the ID of the portable unit contained in the signal transmitted from the portable unit or not;

the controller ~~control unit~~ provided in the in-vehicle unit causing the door lock mechanism to be locked/unlocked if the portable unit authenticating unit judges that the signal is a transmission signal that is transmitted from a predetermined portable unit;

~~encrypting the security data with a cipher key in an encryption unit provided between the controller and the first nonvolatile memory of the in-vehicle unit; and~~

~~storing the encrypted signal into the first nonvolatile memory and storing the cipher key into a second nonvolatile memory,~~

wherein an encryption unit for encrypting the ID of the portable unit with a second cipher key is interposed between the controller and the nonvolatile memory of the in-vehicle unit, and

the ID of the portable unit contained in the signal transmitted from the portable unit is encrypted by the encryption unit with the second cipher key and stored into the nonvolatile memory according to an [[the]] instruction from the

controller when the transmission signal is received from the portable unit after setting the in-vehicle unit into an ID register mode.

6. (Previously Presented) The handling device of security data according to claim 1, wherein the encryption unit decodes encrypted data.

7. (Currently Amended) The handling method ~~device~~ of security data according to claim 5, wherein the second cipher key is stored in another nonvolatile memory, which is not the aforementioned nonvolatile memory.